- wer für Gruppenpostfächer zuständig ist,
- wie mit Datei-Anhängen umgegangen werden soll und
- ob Benutzende die HTML-Darstellung von E-Mails aktivieren dürfen.

Die E-Mail-Sicherheitsrichtlinie SOLLTE ergänzend für die Administrierenden die Einstellungsoptionen der E-Mail-Anwendungen beinhalten, außerdem die Vorgaben für mögliche Zugriffe von anderen Servern auf einen E-Mail-Server. Auch Angaben zu berechtigten Zugriffspunkten, von denen aus auf einen E-Mail-Server zugegriffen werden darf, SOLLTEN in der Richtlinie enthalten sein.

Die E-Mail-Sicherheitsrichtlinie SOLLTE den Umgang mit Newsgroups und Mailinglisten regeln.

APP.5.3.A7 Schulung zu Sicherheitsmechanismen von E-Mail-Clients für Benutzende (S)

Die Institution SOLLTE das Personal darüber aufklären, welche Risiken entstehen, wenn E-Mail-Anwendungen benutzt werden und wie sicher mit E-Mails umgegangen werden kann. Dies SOLLTE zusätzlich zur allgemeinen Schulung und Sensibilisierung geschehen. Die Institution SOLLTE zu den Gefahren sensibilisieren, die entstehen können, wenn E-Mail-Anhänge geöffnet werden. Die Schulungen SOLLTEN ebenfalls darauf eingehen, wie E-Mails von gefälschten Absendeadressen erkannt werden können.

Die Institution SOLLTE davor warnen, an E-Mail-Kettenbriefen teilzunehmen oder zu viele Mailinglisten zu abonnieren.

APP.5.3.A8 Umgang mit Spam durch Benutzende (S) [Benutzende]

Grundsätzlich SOLLTEN die Benutzenden alle Spam-E-Mails ignorieren und löschen. Die Benutzenden SOLLTEN auf unerwünschte E-Mails nicht antworten. Sie SOLLTEN Links in diesen E-Mails nicht folgen. Falls die Institution über ein zentrales Spam-Management verfügt, SOLLTEN die Benutzenden Spam-E-Mails an dieses weiterleiten und die E-Mails danach löschen.

APP.5.3.A9 Erweiterte Sicherheitsmaßnahmen auf dem E-Mail-Server (S)

Die E-Mail-Server einer Institution SOLLTEN eingehende E-Mails mittels des Sender Policy Framework (SPF) und mit Hilfe von DomainKeys Identified Mail (DKIM) überprüfen. Die Institution SOLLTE selbst DKIM und SPF einsetzen, um von ihr versendete E-Mails zu authentisieren.

Wird SPF verwendet, SOLLTEN alle sendeberechtigten E-Mail-Server für eine Domain im SPF-Eintrag angegeben werden. Der SPF-Eintrag SOLLTE den „-all" Parameter enthalten. Der Softfail-Parameter („~") SOLLTE nur zu Testzwecken verwendet werden.

Die Institution SOLLTE Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzen, um festzulegen, wie von ihr versendete E-Mails durch den empfangenden E-Mail-Server überprüft werden sollen. DMARC-Einträge SOLLTEN vorgeben, dass E-Mails im Fehlerfall abgewiesen werden. DMARC-Reporte SOLLTEN regelmäßig ausgewertet werden. Die Institution SOLLTE festlegen, ob DMARC-Reporte über empfangene E-Mails an andere Institutionen versendet werden.

Die Institution SOLLTE die E-Mail-Kommunikation über DANE und MTA-STS absichern.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.5.3.A10 Ende-zu-Ende-Verschlüsselung und Signatur (H)

Die Institution SOLLTE eine Ende-zu-Ende-Verschlüsselung sowie digitale Signaturen für E-Mails einsetzen. Es SOLLTEN nur Protokolle zur Verschlüsselung und Signatur genutzt werden, die dem aktuellen Stand der Technik entsprechen.

APP.5.3.A11 Einsatz redundanter E-Mail-Server (H)

Die Institution SOLLTE redundante E-Mail-Server betreiben. Die redundanten E-Mail-Server SOLLTEN mit geeigneter Priorität in den MX-Records der betroffenen Domains hinterlegt werden. Die Institution SOLLTE festlegen, wie E-Mails zwischen den E-Mail-Servern synchronisiert werden.

APP.5.3.A12 Überwachung öffentlicher Block-Listen (H)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die E-Mail-Server der Institution auf öffentlichen Spam- oder Block-Listen aufgeführt sind.

APP.5.3.A13 TLS-Reporting (H)

Die Institution SOLLTE TLS-Reporting einsetzen. Es SOLLTE festgelegt werden, ob TLS-Reports an andere Institutionen versendet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel 13.2.3 Vorgaben für den Betrieb von E-Mail-Diensten.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF2.3.3 Vorgaben für den Betrieb von E-Mail-Diensten.

Das National Institute of Standards and Technology (NIST) beschreibt in seinen „Guidelines on Electronic Mail Security“ wie E-Mail-Anwendungen sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „BSI TR-03108 Sicherer E-Mail-Transport“ Informationen darüber zur Verfügung, wie E-Mails sicher versendet werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.5.4 Unified Communications und Collaboration (UCC)

1. Beschreibung

1.1. Einleitung

Unified Communications bezeichnet einen Dienst, der verschiedene Kommunikationsdienste in einer Anwendung und in der Regel auch einem Softclient vereint. Damit wird der Anteil der traditionellen Telefonie in der persönlichen digitalen Kommunikation reduziert. Die möglichen Kommunikationswege werden um zusätzliche Dienste wie Video, diverse Formen von Chats und Erreichbarkeitsanzeigen erweitert.

Eine Kommunikationsbeziehung zwischen zwei oder mehr Teilnehmenden wird unabhängig vom benutzten Dienst als Konversation bezeichnet.

Die häufig bei Unified Communications und Collaboration (UCC) genannte Zusammenarbeit (Collaboration) geht noch einen Schritt weiter. Während damit in der Vergangenheit häufig nur Dienste wie Screen Sharing und (digitales) Whiteboarding bezeichnet wurden, stellen UCC-Dienste viele weitere Funktionen zur Verfügung. Insbesondere beim Zusammenarbeiten von Teams hat sich eine Anzahl von Anwendungen etabliert, die häufig als Cloud-Dienst benutzt werden und neben Telefonie, Erreichbarkeitsanzeige, klassischen Chats, Video-Anrufen und Konferenzen auch Team-Chatbereiche sowie gemeinsame Dateiablagen beinhalten. Hinzukommen (offene) Schnittstellen, wodurch zusätzliche Anwendungen integriert werden können, so dass der Gesamtdienst funktional gegebenenfalls sehr umfangreich wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil beim erweiterten Kommunikationsspektrum von UCC-Diensten zu etablieren, ein Bewusstsein für die potenzielle Gefährdungslage dieser Anwendungen zu schaffen und Ansätze zur Vermeidung von Gefährdungen anzubieten.

1.3. Abgrenzung und Modellierung

Der Baustein APP.5.4 *Unified Communications und Collaboration (UCC)* ist auf alle IT-Systeme und Kommunikationsnetze sowie Anwendungen anzuwenden, mit denen UCC-Dienste betrieben werden. Da UCC über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* und NET.3.2 *Firewall* zu berücksichtigen.

Da sich der Geltungsbereich von Kommunikationsdiensten durch UCC zunehmend erweitert, gibt es eine besonders große Zahl von Überschneidungen mit anderen Bausteinen.

Dieser Baustein behandelt die folgenden Inhalte:

- die UCC-Dienste sowie Interaktion und Wechselwirkungen unterschiedlicher Dienste
- die (Soft-) Clients, die bereitgestellt werden, um diese Dienste zu benutzen und deren Funktionsumfang
- die zugehörigen Infrastrukturkomponenten, sofern diese nicht bereits durch andere Bausteine abgedeckt sind
- Themen, die sich aus dem (aus Sicht der Benutzenden) fließenden Übergang zwischen der UCC-Umgebung und weiteren Anwendungen ergeben

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Falls über eine dedizierte TK-Anlage telefoniert wird, muss der Baustein NET.4.1 *TK-Anlagen* angewendet werden.
- Für Voice over IP (VoIP) als ein elementarer Dienst bei UCC-Diensten muss der Baustein NET.4.2 *VoIP* angewendet werden.
- Für die zentralen Server sowie diverse Endgeräte und Clients müssen die Bausteine SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeiner Client* sowie gegebenenfalls spezifische Bausteine angewendet werden.
- Für die zugrundeliegenden Netze muss der Baustein NET.1.1 *Netzarchitektur und -design* angewendet werden.
- Falls UCC-Dienste aus der Cloud bereitgestellt werden, ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.
- Um Dateiablagen abzusichern, die im Rahmen der UCC-Dienste bereitgestellt werden, sind insbesondere die Bausteine APP.3.3 *Fileserver* und SYS.1.8 *Speicherlösungen* anzuwenden.

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Der E-Mail-Dienst ist in der Regel nicht Teil der UCC-Dienste. Hier ist der Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* anzuwenden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.5.4 *Unified Communications und Collaboration (UCC*) von besonderer Bedeutung.

2.1. Eingeschränkte Verfügbarkeit von UCC-Diensten

UCC-Dienste unterliegen häufig erhöhten Anforderungen an die Verfügbarkeit und gleichzeitig hängt die Funktionstüchtigkeit von UCC-Diensten von weiteren IT-Systemen und Anwendungen ab.

Falls die Datennetze, die von UCC-Diensten verwendet werden, nicht voll funktionsfähig sind, kann das die Verfügbarkeit der UCC-Dienste beeinträchtigen. So können beispielsweise Störungen im Datennetz oder bei der Internetverbindung die Qualität der Kommunikation einschränken, was eine verzögerte Sprachverständigung, Artefakte im Videobild oder den Abbruch der Verbindung verursachen kann.

Abhängigkeiten zwischen kritischen IT-Systemen können auch die Funktionsfähigkeit von weiteren Diensten oder Organisationseinheiten behindern. Wenn beispielsweise UCC als Kommunikationsplattform zwingend erforderlich ist, um das Netz wiederaufzubauen, das Netz aber benötigt wird, damit die UCC-Dienste funktionieren, dann blockieren sich beide und können nicht wiederhergestellt werden.

Häufig werden UCC-Dienste als Cloud-Dienst benutzt oder bei einem Dienstleistungsunternehmen betrieben, wodurch Störungen bei externen Netzen oder beim Dienstleistungsunternehmen zu eingeschränkter Verfügbarkeit der UCC-Dienste führen können. Gleiches gilt für den Authentisierungsdienst, über den sich die Benutzenden an den UCC-Diensten anmelden. Fällt der Authentisierungsdienst aus, können die UCC-Dienste oft nicht mehr verwendet werden.

2.2. Unzureichende Planung von UCC

Wenn UCC nicht so geplant wird, wie es auch tatsächlich benutzt werden soll, kann dies Auswirkungen auf die Funktionalität aller UCC-Dienste haben. Werden UCC-Komponenten verändert oder vermehrt benutzt, z. B. durch eine erhöhte Anzahl von Benutzenden, kann eine ursprünglich geeignete Planung unzureichend werden.

Je nach Bereitstellungsart und benutzten Diensten können sich die Anforderungen der UCC-Komponenten an die Netze stark unterscheiden. Eine auf Sprachkommunikation fokussierte UCC-Komponente im eigenen Netz kann beispielsweise andere Anforderungen an Internet- und WAN-Verbindungen stellen als ein Cloud-Dienst, der auch mobil benutzt werden soll. Werden die Netze nicht so geplant, dass sie UCC-Dienste berücksichtigen, sind die UCC-Dienste nicht ausreichend benutzbar.

Entsprechende Gefährdungen gibt es auch für die zu berücksichtigenden Endgeräte. Besonders die Videokommunikation und die zugehörigen Funktionen stellen zum Teil sehr hohe Anforderungen an die Clients. Insbesondere

bei Thin Clients kann dies zu Problemen führen, da UCC-Dienste häufig ganz oder teilweise auf dem Endgerät ausgeführt werden, um Kommunikationsdatenströme zu optimieren. Clients mit unzureichender Rechenleistung können beispielsweise Aussetzer oder Artefakte bei der Videokommunikation bedingen.

2.3. Fehlerhafte Konfiguration von UCC

Eine große Zahl von Funktionen und Diensten bedeutet oft auch eine Vielzahl von Konfigurationsmöglichkeiten. Dabei können Fehlkonfigurationen auftreten.

Benutzende können oder müssen ihre UCC-Clients teilweise selbst konfigurieren. Dies kann Benutzende aufgrund der Vielzahl von Konfigurationsmöglichkeiten überfordern und fehlerhafte Konfigurationen verursachen. Wenn beispielsweise im Büro und im Homeoffice verschiedene Headsets verwendet werden, muss die Konfiguration gegebenenfalls angepasst werden. Fehlkonfigurationen können dazu führen, dass Benutzende in Besprechungen nicht hör- oder sichtbar sind oder selbst keinen Ton hören. Darüber hinaus können ungewollt Informationen preisgegeben werden, wenn Raumsysteme so konfiguriert sind, dass eingehende Kommunikationsanfragen automatisch angenommen werden.

Ebenso können durch ein unzureichendes Identitäts- und Berechtigungskonzept Fehler auftreten, wenn UCC-Dienste konfiguriert werden. Administrierende, die im Rahmen der Einrichtung von neuen Konten ebenfalls zentrale Routing-Einstellungen ändern, können hierdurch eine gravierende Fehlkonfiguration verursachen. Diese kann dazu führen, dass Daten verloren gehen, oder der UCC-Dienst ausfällt.

Zu den Fehlkonfigurationen durch ein unzureichendes Identitäts- und Berechtigungskonzept gehören auch unzureichend eingeschränkte Berechtigungen von externen Teilnehmenden. Können diese beispielsweise unberechtigt auf Inhalte von Konversationen zugreifen, so können Informationen abfließen oder manipuliert werden.

2.4. Unbefugte oder missbräuchliche Benutzung der Administrationsrechte eines UCC-Dienstes

Durch die zugewiesenen Administrationsrechte können Administrierende die UCC-Dienste gegebenenfalls tiefgreifend ändern. Werden Administrationsrechte unbefugt oder missbräuchlich benutzt, kann dies weitreichende Folgen haben. Beispielsweise können Administrationsrechte dazu benutzt werden, um einen privaten Bereich, wie einen Chat oder eine Dateiablage, der ursprünglich nur für einen begrenzten Personenkreis zugänglich war, für alle Benutzenden des UCC-Dienstes freizugeben. Hierdurch können schützenswerte Informationen durch unbefugte Personen eingesehen und gegebenenfalls verändert werden.

Weiterhin können durch vorsätzlich veränderte Routing-Konfigurationen die UCC-Dienste nicht oder nur eingeschränkt zur Verfügung stehen. Falls beispielsweise sämtliche ausgehende Anrufe durch zentrale IT-Systeme blockiert werden, kann der Dienst Telefonie nicht mehr benutzt werden.

2.5. Preisgabe von schützenswerten Informationen

Moderne UCC-Clients verfügen über eine Vielfalt an Funktionen und sind daher für viele Benutzende unübersichtlich. Dies begünstigt Fehlbedienungen, die dazu führen können, dass Informationen nicht regelkonform weitergegeben werden. Wird versehentlich ein falscher Kontakt ausgewählt, erhält dieser gegebenenfalls per Chat ungewollt schützenswerte Informationen. Ein weiteres Szenario ist, ungewollt Informationen bei einer Bildschirmfreigabe preiszugeben, wenn beispielsweise versehentlich der E-Mail-Client statt der vorgesehenen Präsentation freigegeben wird.

Vielen Benutzenden ist nicht bewusst, dass die UCC-Dienste Daten, die beispielsweise innerhalb von privaten Chats gesendet werden, in einer Cloud abspeichern. So können unbewusst Ablagerichtlinien der Institution verletzt werden. Gleiches gilt für Dateien, in denen Konversationen aufgezeichnet wurden.

Teambereiche verfügen zwar in der Regel über einen definierten Kreis von Benutzenden und entsprechende Zugriffsbeschränkungen, jedoch ist vielen Benutzenden nicht bewusst, dass die Zugriffsrechte und Mitgliedschaften nachträglich modifiziert werden können. Dadurch können weitere Personen auf alle zuvor dort abgelegten Dateien zugreifen. Darüber hinaus werden häufig öffentliche Teambereiche erstellt, denen weitere Personen ohne explizite Erlaubnis beitreten können. Dadurch können gegebenenfalls Daten von unberechtigten Personen eingesehen werden. Beispielsweise kann ein Teambereich eines Projekts ausschließlich aus internen Benutzenden bestehen. Teilnehmende laden nun interne Dokumente hoch, da alle Teammitglieder intern sind. Wenn im weiteren Projektverlauf externe Personen in den Bereich eingeladen werden, können sie auf alle bisherigen Dokumente zugreifen.

2.6. Preisgabe von personenbezogenen Informationen

UCC-Dienste erheben an vielen Stellen Daten, die auch anderen Benutzenden angezeigt werden. Dies kann dazu führen, dass personenbezogene Informationen ungewollt preisgegeben werden.

Unter anderem kann die Verfügbarkeit von Benutzenden sichtbar sein. Auch Zeitstempel an Beiträgen in Chats bis hin zu umfangreichen Auswertungen über Gespräche, Aktivitäten oder Inhalte für einzelne Benutzende können Teil einer UCC-Komponente sein. Dabei können sogar Personenprofile durch die UCC-Dienste gebildet werden. Auch Personen ohne erweiterte Berechtigungen erhalten häufig Zugriff auf diese Auswertungen. Dadurch können sie Rückschlüsse auf Arbeitszeiten und -inhalte sowie persönliche Beziehungen anderer Personen ziehen und diese beispielsweise zur Leistungsüberwachung verwenden.

Werden bei mobilem Arbeiten virtuelle Konferenzen benutzt, können ungewollt private Informationen an die Teilnehmenden der Konferenz übermittelt werden. Dazu zählen beispielsweise Personen, die durch das Videobild laufen, persönliche Gegenstände im Hintergrund einer Videoübertragung oder Geräusche und Stimmen aus dem privaten Umfeld.

2.7. Wechselwirkungen bei UCC-Diensten

UCC-Dienste können untereinander Wechselwirkungen verursachen, welche die Funktionalität einschränken.

Um das Benutzungserlebnis zu verbessern, werden verschiedene Dienste häufig in einer Benutzungsoberfläche verknüpft. Dies kann jedoch zu Abhängigkeiten zwischen den Diensten führen. Wird beispielsweise der Videokonferenzdienst in eine Oberfläche zur Teamkollaboration integriert, kann der Videodienstes nicht mehr verwendet werden, falls die Oberfläche ausfällt.

UCC-Dienste benutzen häufig gemeinsame Ressourcen. Dies kann zu Konflikten führen, welche die Funktionalität beeinträchtigen. Werden Headsets beispielsweise von einer Telefonie- und einer Videokonferenzanwendung gleichzeitig verwendet, können die Headsets durch eine Anwendung blockiert werden und dann nicht mehr für die andere Anwendung zur Verfügung stehen.

Manche Anwendungen haben sehr hohe Ressourcenanforderungen. Wenn mehrere UCC-Dienste gleichzeitig auf einem IT-System ausgeführt werden, kann dies dazu führen, dass der Client überfordert ist und das IT-System ausfällt oder abstürzt. Wenn beispielsweise mehrere Videokonferenzanwendungen parallel im Hintergrund ausgeführt werden, kann die resultierende Auslastung des Arbeitsspeichers den Client stark beeinträchtigen.

2.8. Zugriff auf Applikationen oder Ressourcen durch Freigabe der Steuerung

Werden den Teilnehmenden innerhalb einer Konversation Desktop- oder Bildschirminhalte angezeigt, kann die Steuerung durch den Freigebenden an andere Benutzende übertragen werden. Dies kann jedoch dazu führen, dass der Freigebende die Kontrolle über weitere Handlungen verliert.

Da die Funktion zwar häufig vorhanden ist, in der Regel aber nur selten benutzt wird, sind viele Benutzende mit der Bedienung nicht vertraut, akzeptieren die Freigabe und verlieren dann die Kontrolle über ihren Client. Beispielsweise können Benutzende die Steuerung ihrer Maus freigeben, ohne zu wissen, wie die Freigabe beendet werden kann. Dadurch können Teilnehmende der Konversation möglicherweise auf weitere Anwendungen des Clients zugreifen.

2.9. Vorspiegelung falscher Identitäten

Dadurch, dass neue UCC-Dienste eingeführt werden und Externe neue Möglichkeiten erhalten, Kontakt aufzunehmen, ergeben sich neue Wege für Angreifende, die sich als vertrauenswürdige Kommunikationspartner und -partnerin ausgeben wollen, um so an vertrauliche Informationen zu gelangen.

Die Komplexität von UCC-Diensten erhöht die Wahrscheinlichkeit für Fehlbedienungen oder unbewusste Verletzungen von Sicherheitsrichtlinien durch die Benutzenden. Hyperlinks zu schädlichen Inhalten können beispielsweise geöffnet werden, weil die UCC-Dienste als interne Plattform mit erhöhter Vertrauenswürdigkeit wahrgenommen werden.

Häufig sind sich die Benutzenden nicht darüber bewusst, dass sie auch von unbekannten Externen kontaktiert werden können. Dadurch sind sie anfälliger für Social Engineering, beispielsweise über einen Chat oder eine Einladung zu einer Konversation.

Weiterhin können Angreifende ihre angezeigten Namen, ihre Stimme oder ihr Aussehen manipulieren. Dadurch kann sich zum Beispiel eine externe Person über die vermeintlich interne Kommunikationsplattform als vorgesetzte Person ausgeben, um so vertrauliche Informationen oder Dokumente direkt über den Chat zu erhalten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.4 *Unified Communications und Collaboration (UCC)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.5.4.A1 Planung von UCC (B)

Es MUSS umfassend und detailliert geplant werden, wie und für welchen Zweck UCC eingesetzt werden soll. Die Planung MUSS insbesondere die Wechselwirkungen der UCC-Dienste berücksichtigen und mindestens folgende Aspekte beinhalten:

- Einsatzzwecke der vorgesehenen UCC-Dienste
- Funktionale Anforderungen an UCC als Gesamtheit und an die einzelnen UCC-Dienste
- Anforderungen zur Absicherung von UCC
- Festlegung zu Informationen und Daten, die über UCC übertragen werden dürfen
- Analyse der Kommunikation und der Abhängigkeiten von UCC-Diensten untereinander
- Produkt- und Dienstauswahl ausgehend von den definierten Anforderungen
- Aufstellen von organisatorischen Regelungen, um die UCC-Dienste zu benutzen

Bei der Planung MUSS berücksichtigt werden, wie UCC in die IT-Infrastruktur der Institution integriert wird. Hierbei MUSS insbesondere betrachtet werden, ob und wie die Systeme der UCC-Dienste innerhalb des Netzes separiert werden sollen und welche Schnittstellen zu weiteren benutzten Anwendungen notwendig sind.

APP.5.4.A2 Berücksichtigung von UCC in der Netzplanung (B)

Bevor UCC-Dienste eingeführt werden, MUSS geprüft werden, ob das Netz die UCC-spezifischen Leistungsparameter erfüllt. Falls die Leistungsparameter nicht erfüllt werden, MUSS festgelegt werden, wie hiermit umgegangen wird.

Sollen UCC-Dienste benutzt werden, SOLLTEN im Rahmen der allgemeinen Netzplanung insbesondere folgende Aspekte berücksichtigt werden:

- Erfüllung der UCC-spezifischen Leistungsparameter wie Paketverlust, Jitter und Latenz
- Netzkapazitäten (Bandbreite) für die festgelegte Benutzung der UCC-Dienste wie Videokonferenzen

- Berücksichtigung von Power over Ethernet (PoE) für stationäre Endgeräte
- Verfügbarkeit von WLAN für mobile Endgeräte

Falls die UCC-Dienste erweitert werden, SOLLTEN diese Aspekte erneut geprüft werden.

APP.5.4.A3 Initiales und regelmäßiges Testen der UCC-Dienste (B)

Für die UCC-Dienste MÜSSEN initial Tests durchgeführt werden, die verifizieren, dass die UCC-Komponenten untereinander und mit anderen UCC-Diensten interferenzfrei funktionieren. Ebenfalls MÜSSEN Tests mit ausgewählten Benutzenden durchgeführt werden, um insbesondere Wechselwirkungen mit anderen Anwendungen zu überprüfen.

Diese Tests SOLLTEN wiederholt werden, wenn die UCC-Dienste erweitert oder verändert werden.

Zusätzlich SOLLTE die Konfiguration der UCC-Dienste in regelmäßigen Abständen auf Plausibilität und Konformität für die festgelegten Einsatzzwecke überprüft werden.

APP.5.4.A4 Deaktivierung nicht benötigter Funktionen und Dienste (B)

UCC-Dienste DÜRFEN NUR mit dem geringsten notwendigen Funktionsumfang betrieben werden. Die verfügbaren Funktionen und Dienste MÜSSEN entsprechend der definierten Einsatzzwecke ausgewählt werden. Dabei MÜSSEN gegebenenfalls auftretende Wechselwirkungen zwischen den verschiedenen Komponenten eines UCC-Dienstes berücksichtigt werden. Außerdem MÜSSEN insbesondere die folgenden Dienste und Funktionen auf Notwendigkeit geprüft und gegebenenfalls deaktiviert oder eingeschränkt werden:

- Speicherung von personenbezogenen Daten durch die UCC-Komponenten
- Zugriff und Verarbeitung von personenbezogenen Daten durch Benutzende und den UCC-Dienst
- Benutzbarkeit von Funktionen wie Chat, Erreichbarkeitsstatus, Dateiablagen oder Team-Bereiche durch externe Teilnehmende
- Senden von Daten und Dateien an externe UCC-Dienste

Konversationsbezogene Log-Daten DÜRFEN NUR in minimal notwendigem Umfang gespeichert werden. Funktionen und Dienste, die auf (dauerhaft) gespeicherte Log-Daten zugreifen, MÜSSEN auf ihre Notwendigkeit geprüft und gegebenenfalls deaktiviert werden.

APP.5.4.A5 Rollen- und Berechtigungskonzept für UCC (B)

Das Rollen- und Berechtigungskonzept MUSS um UCC-spezifische Definitionen von Rollen und Berechtigungen ergänzt werden. Solche Definitionen MÜSSEN sowohl für alle internen Benutzenden als auch für die externen Benutzenden getroffen werden. Es MÜSSEN folgende Aspekte berücksichtigt werden:

- Berechtigungen zur zielgerichteten Benutzung von UCC-Diensten gemäß festgelegter Einsatzzwecke
- Berechtigungen zur Anpassung der Konfiguration von Konversationen
- Berechtigungen für spezielle Funktionen von UCC-Diensten wie Aufzeichnung von Konversationen und Zugriff auf Dateiablagen eines UCC-Dienstes

Darüber hinaus MÜSSEN die Berechtigungen der Konten ebenfalls auf das notwendige Minimum reduziert werden. Dienste, die nur für einen Teil der Benutzenden zur Verfügung stehen, DÜRFEN NICHT für die restlichen Benutzenden zugänglich sein.

Zudem SOLLTEN nur Benutzende mit einer entsprechenden Berechtigung auf Daten wie Aufzeichnungen oder Dateiablagen zugreifen können.

Die Festlegungen MÜSSEN festgehalten, regelmäßig und anlassbezogen geprüft und aktualisiert werden.

APP.5.4.A6 Verschlüsselung von UCC-Daten (B)

Sämtliche Kommunikation über unzureichend vertrauenswürdige Netze MUSS mit sicheren Verfahren verschlüsselt werden, sofern dies durch die jeweilige UCC-Komponente unterstützt wird. Falls eine Verschlüsselung für einzelne UCC-Komponenten oder einzelne Konversationen nicht möglich ist, MUSS die Festlegung, welche Informationen über diese UCC-Komponenten übertragen werden dürfen, geprüft und gegebenenfalls angepasst werden.

Insbesondere MUSS bei anwendungsübergreifender Kommunikation festgelegt werden, für welche Konversationen die Medienströme und die Signalisierung und welche weiteren Daten wie Chat oder Dateitransfer verschlüsselt übertragen werden müssen.

Dateiablagen, die persistente personenbezogene oder vertrauliche Daten enthalten, MÜSSEN mit Hilfe von sicheren Verschlüsselungsmechanismen abgesichert werden. Hierbei MÜSSEN sowohl interne Dateiablagen der UCC-Dienste als auch über Schnittstellen angebundene externe Dateiablagen berücksichtigt werden.

Die Benutzenden MÜSSEN zudem über den Status der Verschlüsselung innerhalb von Konversationen informiert werden.

APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste (B)

Konversationen, die mit Hilfe von UCC durchgeführt werden, MÜSSEN abgesichert werden. Hierbei MÜSSEN folgende Aspekte berücksichtigt werden:

- Auswahl der Teilnehmenden entsprechend dem Inhalt der Konversation
- zusätzliche Absicherung von geplanten Konversationen über Mechanismen wie PIN oder ein Passwort
- Zuweisung von Moderationsrechten an ausgewählte Benutzende der einladenden Institution
- Regelungen zum Umgang mit Aufzeichnungen von Konversationen
- Regelungen für Endgeräte, die von mehreren Benutzenden verwendet werden

Die Benutzenden MÜSSEN über Funktionen informiert werden, über die Konversationen abgesichert werden können. Ebenso MÜSSEN die Benutzenden dafür sensibilisiert werden, wie die UCC-Dienste sicher benutzt werden, insbesondere für externe Chats oder Videokonferenzen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.5.4.A8 Einsatz eines Session Border Controller am Provider-Übergang (S)

Für die UCC-Kommunikation über eingeschränkt vertrauenswürdige Netze SOLLTE mindestens für Sprachdienste ein Session Border Controller (SBC) am Netzübergang bzw. beim Übergang zum SIP-Provider eingesetzt werden. Der SBC SOLLTE als Verschlüsselungsendpunkt die Signalisierung und die Medienströme terminieren. Der SBC SOLLTE für die Signalisierung und die Medienströme Filterfunktionen unterstützen, die die jeweiligen Konversationen zusätzlich absichern.

APP.5.4.A9 Sichere Konfiguration von UCC (S)

Um UCC sicher zu konfigurieren, SOLLTEN mindestens die folgenden Aspekte berücksichtigt werden:

- Verschlüsselung von Signalisierungs- und Mediendaten auch auf vertrauenswürdigen Übertragungsstrecken
- Absicherung von gespeicherten Daten, insbesondere Festlegung für Zugriffsberechtigung auf Aufzeichnungen von Konversationen
- Einschränkung der zur Verfügung stehenden Dienste auf ausschließlich interne Benutzende
- Einschränkung der Übertragung von Erreichbarkeitsinformationen

Gespeicherte Daten SOLLTEN verschlüsselt werden. Auf gespeicherte Daten SOLLTEN Benutzende nur nach vorheriger Authentisierung zugreifen können.

Der IT-Betrieb SOLLTE sichere Einstellungen vorgeben, die verwendet werden, wenn Konversationen erstellt werden. Für textbasierte Konversationen SOLLTE ein Malware-Schutz aktiviert werden.

Die Umsetzung SOLLTE festgehalten, regelmäßig und anlassbezogen auf Einhaltung der Vorgaben geprüft und angepasst werden.

APP.5.4.A10 Absicherung und Einschränkung von Auswertungen von Inhalten (S)

Die Art einer (automatischen) Auswertung von Konversationsinhalten SOLLTE schon im Vorfeld sorgfältig geprüft werden und ihr Nutzen gegen den Schutzbedarf abgewogen werden. Es SOLLTE die Möglichkeit bestehen, entsprechende Funktionen entweder vollständig oder pro Konversation zu deaktivieren und eine inhaltliche Auswertung der Kommunikation zu verhindern. Besondere Beachtung SOLLTEN KI-Funktionen und die Übertragung von Daten an Onlinedienste erhalten.

Werden Inhalte über den Zweck der Konversation hinausgehend ausgewertet, MUSS dazu auch eine Zustimmung der an der Konversation teilnehmenden Personen eingeholt werden.

Werden während der Auswertung von Konversationen persistente Daten erzeugt, SOLLTEN für diese geeignete Schutzmaßnahmen umgesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.5.4.A11 Sicherstellung der Verfügbarkeit von Kommunikationsdiensten (H)

Die Verfügbarkeit von UCC-Diensten SOLLTE insbesondere durch folgende technische Maßnahmen sichergestellt werden:

- redundante Auslegung zentraler Server und Dienste
- Benutzung von Call Admission Control (CAC) zur Qualitätssicherung von Telefonie und Video-Diensten
- möglichst autark funktionierende UCC-Dienste

Darüber hinaus SOLLTE bei Cloud-basierten UCC-Diensten der Cloud-Provider sowie der Internet-Provider ausfallsicher an das eigene Netz angebunden werden.

Zudem SOLLTE ein SIP-Provider, der Rufnummern bereitstellt und den Übergang ins öffentliche Telefonnetz bildet, hochverfügbar an das eigene Netz angebunden werden.

Die Verfügbarkeit SOLLTE durch ein Monitoring der UCC-Dienste überwacht werden.

APP.5.4.A12 Einbindung von UCC in die Notfallplanung (H)

Ausgehend von einer Business Impact Analyse SOLLTE geprüft werden, welche UCC-Dienste in der Notfallplanung berücksichtigt werden sollen. Hierbei SOLLTEN in Notfallsituationen für einzelne UCC-Dienste alternative Anwendungen bereitgestellt werden. Insbesondere SOLLTE für die Benutzenden die Erreichbarkeit von wichtigen Diensten wie der Notruf gewährleistet werden.

Zudem SOLLTE ein Notfallplan für die UCC-Dienste erstellt werden, in dem notwendige Konfigurationen sowie Routing-Anpassungen, die über den Telefonie-Provider realisiert werden, behandelt werden.

Ebenso SOLLTE der Wiederanlauf der UCC-Komponenten und –Dienste unter Berücksichtigung der Wechselwirkungen innerhalb der UCC-Dienste festgelegt werden.

APP.5.4.A13 Sichere Administration von SIP-Trunks (H)

Wenn SIP-Trunks administriert werden, SOLLTE für folgende Tätigkeiten ein 4-Augen-Prinzip angewendet werden:

- Änderungen an Routing-Konfigurationen
- Änderungen an Parametern, die im Rahmen von Call Admission Control benutzt werden
- Änderungen hinsichtlich der Verschlüsselung sowohl in Richtung des eigenen Netzes als auch in Richtung des Provider-Netzes
- Änderungen an weiteren sicherheitsrelevanten Konfigurationen wie der lokalen Speicherung von Verbindungsdaten

APP.5.4.A14 Ende-zu-Ende-Verschlüsselung (H)

Für UCC-Kommunikation SOLLTE eine sichere Ende-zu-Ende-Verschlüsselung benutzt werden. Die Ende-zu-Ende-Verschlüsselung SOLLTE sich sowohl auf die Signalisierung als auch auf die Mediendaten von Audio- und Videokommunikation mit zwei oder mehr Teilnehmenden erstrecken.

Bei Konversationen zwischen UCC-Diensten von verschiedenen Herstellenden SOLLTEN die übertragenen Informationen eingeschränkt werden, sofern eine Ende-zu-Ende-Verschlüsselung nach Stand der Technik nicht möglich ist.

APP.5.4.A15 Einschränkung von KI-Funktionen (H)

Die Benutzung von KI-Funktionen SOLLTE deaktiviert oder auf ein Minimum reduziert werden. Ist eine permanente Deaktivierung nicht möglich oder erwünscht, SOLLTE festgelegt werden, dass Benutzende der UCC-Dienste zu Beginn einer Konversation zielgerichtet KI-Funktionen deaktivieren, falls dies möglich ist.

APP.5.4.A16 Einsatz eines SBC an weiteren Netzübergängen (H)

Ergänzend zu einem SBC am Netzübergang zum Provider, SOLLTEN weitere SBC an internen Netzübergängen eingesetzt werden. Hierbei SOLLTEN insbesondere Netzübergänge zwischen Netzsegmenten mit unterschiedlichem Schutzbedarf berücksichtigt werden.

Der SBC SOLLTE sicherstellen, dass die Verschlüsselungsmechanismen an den SBC-gesicherten Netzsegmentübergängen anforderungskonform realisiert werden.

APP.5.4.A17 Einschränkung der Benutzung von UCC-Diensten (H)

Folgende Aspekte SOLLTEN mindestens berücksichtigt werden, um die UCC-Dienste sowie die übertragenen Daten zusätzlich abzusichern:

- Einschränkung der Dienste entsprechend des Schutzbedarfs der übertragenen Informationen
- Benutzung einer Multi-Faktor-Authentisierung für Benutzende
- Deaktivierung von Funktionen für externe Benutzende
- Deaktivierung der Speicherung von Metadaten
- Einschränkung der Sichtbarkeit von kommunikationsbezogenen Daten für Administrierende

Darüber hinaus SOLLTEN zusätzliche technische und organisatorische Vorkehrungen getroffen werden, um Konversationen über die Vergabe von PINs bzw. Passwörtern hinaus abzusichern.

APP.5.4.A18 Einbindung von UCC in ein Sicherheitsmonitoring (H)

Die zentralen UCC-Komponenten SOLLTEN durch ein Sicherheitsmonitoring überwacht werden. Dies SOLLTE mindestens für Komponenten umgesetzt werden, die wie Multipoint Control Units Verschlüsselungsendpunkte realisieren oder die wie SBCs an Vertrauensgrenzen positioniert sind.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen UCC-Komponenten hierin eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für die Auswahl von Verschlüsselungsverfahren und Schlüssellängen sollte die technische Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI beachtet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.6 Allgemeine Software

1. Beschreibung

1.1. Einleitung

Dieser Baustein fasst jegliche Software unter dem Begriff Allgemeine Software zusammen, unabhängig davon, ob es sich um eine Textverarbeitung, ein Betriebssystem, eine mobile Kommunikations-App, eine individuell entwickelte Software oder ein verteiltes Content-Management-System handelt.

Dabei durchläuft in der Regel jegliche Software einen Lebenszyklus, der die Planung, Anforderungserhebung, Beschaffung, Software-Tests inklusive Freigabe, Installation in Produktivumgebung, Schulung, Betrieb, Updates und Änderungsmanagement sowie Außerbetriebnahme mitsamt Deinstallation umfasst. Dieser Lebenszyklus kann je nach Anwendungskontext variieren, sodass bei einzelnen Anwendungen noch weitere individuelle Zwischenschritte dazu kommen können und auch der Umfang der einzelnen Schritte schwankt.

Allerdings treten bei den aufgeführten Zwischenschritten immer wiederkehrende Aspekte der Informationssicherheit auf, die auf jegliche Art von Software angewendet werden können.

1.2. Zielsetzung

Der Baustein zeigt auf, welche Sicherheitsanforderungen zu erfüllen sind, damit allgemeine Software über den gesamten Lebenszyklus hinweg sicher eingesetzt werden kann. Übergeordnetes Ziel ist dabei, die Software und die hiermit verarbeiteten Informationen zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.6 *Allgemeine Software* ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden. Ausgenommen hiervon sind Betriebssysteme, die auf geschlossenen Systemen wie IoT-Geräten, Routern, Druckern oder eingebetteten Systemen ausgeführt werden. Häufig wird Software gebündelt ausgeliefert (z. B. Office Suites oder Betriebssysteme mit umfangreich integrierten Boardwerkzeugen) oder um Plug-ins, Add-ons oder vergleichbares erweitert. In solchen Fällen kann der Baustein auf das gesamte Softwarebündel einmal angewendet werden.

Dieser Baustein befasst sich nur mit standardisierten und generischen Verfahrensweisen im Lebenszyklus von Software. Es werden keine konkreten Empfehlungen beschrieben, wie Software im Einzelnen konfiguriert und wie sie durch individuelle Schutzmechanismen auf den eingesetzten IT-Systemen abgesichert werden soll. Hierzu sind die spezifischen Bausteine der APP-Schicht anzuwenden.

Die Zwischenschritte Freigabe (inklusive Software-Tests) sowie Patch- und Änderungsmanagement werden nicht in diesem Baustein behandelt, sondern in den Bausteinen OPS.1.1.6 *Software-Tests und -Freigaben* sowie OPS.1.1.3 *Patch- und Änderungsmanagement*.

Können Anforderungen an Software nicht von einem fertigen Softwareprodukt erfüllt werden, indem z. B. die Konfiguration angepasst wird, sondern es wird ein individuell entwickeltes Produkt benötigt, dann muss der Baustein APP.7 *Entwicklung von Individualsoftware* ergänzend modelliert werden.

Software und die damit verbundenen Daten müssen häufig auch in Notfällen verfügbar sein. Erste Überlegungen hierzu zeigt der Baustein DER.4 *Notfallmanagement* auf.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.6 *Allgemeine Software* von besonderer Bedeutung.

2.1. Ungeeignete Auswahl von Software

Für viele Anwendungszwecke und Einsatzmöglichkeiten werden die unterschiedlichsten Software-Lösungen auf dem Markt angeboten. Wird eine unpassende Software, die nicht den Anforderungen der Institution entspricht, ausgewählt, dann kann der Betrieb erheblich gestört werden. Dateiformate könnten zum Beispiel nicht mit bereits eingesetzten Programmen kompatibel sein oder neue Produkte einen zu geringen Funktionsumfang haben. Das kann zu Leistungsverlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

Insbesondere wenn die Software nicht die Sicherheitsanforderungen der Institution erfüllt, könnten die mit der Software verarbeiteten Daten offengelegt oder manipuliert werden, z. B. wenn Login-Funktionen von Anwendungen nicht für die geplante Einsatzumgebung in einem offenen Datennetz konzeptioniert worden sind.

2.2. Offenlegung schützenswerter Informationen durch fehlerhafte Konfiguration

Ist eine Software fehlerhaft konfiguriert, können unbeabsichtigt schützenswerte Informationen offengelegt werden, z. B. wenn nicht benötigte Funktionen noch aktiviert sind, wie Cloud-Backup-Funktionen, die Daten ungewollt in eine Cloud synchronisieren. Hierdurch könnten sensible Daten von unbefugten Dritten eingesehen und offengelegt werden.

Das kann zu finanziellen Einbußen führen oder die Reputation einer Institution schädigen. Zusätzlich könnte die Institution auch gegen geltendes Recht verstoßen, z. B. wenn personenbezogene Daten offengelegt werden.

2.3. Bezug von Software aus unzuverlässiger Quelle

Wird Software aus unzuverlässigen Quellen bezogen, ist nicht sichergestellt, dass eine unveränderte Originalversion der Software eingesetzt wird. Anstelle dessen könnte eine defekte oder kompromittierte Version der Software bezogen worden sein. Dies gilt auch für Erweiterungen, wie Plug-ins oder Add-ons. Wird kompromittierte Software installiert, kann Schadcode in der Institution verteilt werden. Außerdem ist es möglich, dass die Software nicht wie vorgesehen funktioniert. Darüber hinaus kann die Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

2.4. Sicherheitslücken durch mangelhafte Wartung

Sicherheitslücken und Software-Schwachstellen können prinzipiell über den gesamten Nutzungszeitraum von Software auftreten. Das kann dazu führen, dass die Informationssicherheit der mit der Software verarbeiten Daten gefährdet ist, indem z. B. Login-Funktionen umgangen oder Verschlüsselungen gebrochen werden können.

Sicherheitslücken und Schwachstellen können insbesondere dann nicht zeitnah behoben werden, wenn kein geeigneter Wartungsvertrag mit dem herstellenden oder anbietenden Unternehmen geschlossen wurde oder die Software schlicht über den Wartungszeitraum hinaus verwendet wird. Auch können Verstöße gegen die Lizenzbestimmungen dazu führen, dass z. B. (Auto-)Update-Mechanismen deaktiviert werden und somit die Software nicht mehr gewartet wird.

2.5. Datenverlust durch fehlerhafte Nutzung von Software

Durch falsch benutzte Software können Mitarbeitende Daten versehentlich löschen oder so verändern, dass diese unbrauchbar werden. Dadurch können ganze Geschäftsprozesse blockiert werden. Auch wenn Funktionen zur Verschlüsselung fehlerhaft benutzt werden, könnten die Daten zwar noch vorhanden sein, aber nicht mehr entschlüsselt werden. In diesem Fall können die Daten nicht mehr oder nur noch mit erhöhtem Aufwand wiederhergestellt werden.

2.6. Mangelhafte Ressourcen für die Ausführung von Software

Falls IT-Systeme über ungenügend Ressourcen verfügen, um die Software auszuführen, kann das die Bearbeitungs- und Reaktionszeit für die Benutzende erheblich erhöhen. Im schlimmsten Fall kann die Software auf solch einem System nicht ausgeführt werden. Das kann Geschäftsprozesse erheblich unterbrechen.

2.7. Nichtbeachtung von Anforderungen der Benutzenden

Unabhängig davon, ob eine Software die funktionalen Anforderungen erfüllt, kann sie von den Benutzenden nicht akzeptiert werden, wenn sie z. B. umständlich und kompliziert zu bedienen ist. Dies kann wiederum dazu führen, dass Benutzende auf alternative Formen der Bearbeitung zurückgreifen und dafür anderweitige IT-Systeme oder Software zweckentfremden. So könnten z. B. private IT-Systeme ohne Abstimmung mit dem IT-Betrieb eingesetzt werden. Diese alternativen Formen der Bearbeitung entstehen dabei selten unter Gesichtspunkten der Informationssicherheit und stellen somit ein erhöhtes Risiko dar.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.6 *Allgemeine Software* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Beschaffungsstelle

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.6.A1 Planung des Software-Einsatzes (B) [Fachverantwortliche]

Bevor eine Institution eine (neue) Software einführt, MUSS sie entscheiden,

- wofür die Software genutzt und welche Informationen damit verarbeitet werden sollen,
- wie die Benutzenden bei der Anforderungserhebung beteiligt und bei der Einführung unterstützt werden sollen,
- wie die Software an weitere Anwendungen und IT-Systeme über welche Schnittstellen angebunden wird,
- auf welchen IT-Systemen die Software ausgeführt werden soll und welche Ressourcen zur Ausführung der Software erforderlich sind, sowie
- ob sich die Institution in Abhängigkeit zu einem Hersteller oder einer Herstellerin begibt, wenn sie diese Software einsetzt.

Hierbei MÜSSEN bereits Sicherheitsaspekte berücksichtigt werden. Zusätzlich MUSS die Institution die Zuständigkeiten für fachliche Betreuung, Freigabe und betriebliche Administration schon im Vorfeld klären und festlegen. Die Zuständigkeiten MÜSSEN dokumentiert und bei Bedarf aktualisiert werden.

APP.6.A2 Erstellung eines Anforderungskatalogs für Software (B) [Fachverantwortliche]

Auf Basis der Ergebnisse der Planung MÜSSEN die Anforderungen an die Software in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog MUSS dabei die grundlegenden funktionalen Anforderungen umfas-

sen. Darüber hinaus MÜSSEN die nichtfunktionalen Anforderungen und hier insbesondere die Sicherheitsanforderungen in den Anforderungskatalog integriert werden.

Hierbei MÜSSEN sowohl die Anforderungen von den Fachverantwortlichen als auch vom IT-Betrieb berücksichtigt werden. Insbesondere MÜSSEN auch die rechtlichen Anforderungen, die sich aus dem Kontext der zu verarbeitenden Daten ergeben, berücksichtigt werden.

Der fertige Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen abgestimmt werden.

APP.6.A3 Sichere Beschaffung von Software (B) [Beschaffungsstelle]

Wenn Software beschafft wird, MUSS auf Basis des Anforderungskatalogs eine geeignete Software ausgewählt werden. Die ausgewählte Software MUSS aus vertrauenswürdigen Quellen beschafft werden. Die vertrauenswürdige Quelle SOLLTE eine Möglichkeit bereitstellen, die Software auf Integrität zu überprüfen.

Darüber hinaus SOLLTE die Software mit einem geeigneten Wartungsvertrag oder einer vergleichbaren Zusage des herstellenden oder anbietenden Unternehmens beschafft werden. Diese Verträge oder Zusagen SOLLTEN insbesondere garantieren, dass auftretende Sicherheitslücken und Schwachstellen der Software während des gesamten Nutzungszeitraums zeitnah behoben werden.

APP.6.A4 Regelung für die Installation und Konfiguration von Software (B) [Fachverantwortliche]

Die Installation und Konfiguration der Software MUSS durch den IT-Betrieb so geregelt werden, dass

- die Software nur mit dem geringsten notwendigen Funktionsumfang installiert und ausgeführt wird,
- die Software mit den geringsten möglichen Berechtigungen ausgeführt wird,
- die datensparsamsten Einstellungen (in Bezug auf die Verarbeitung von personenbezogenen Daten) konfiguriert werden sowie
- alle relevanten Sicherheitsupdates und -patches installiert sind, bevor die Software produktiv eingesetzt wird.

Hierbei MÜSSEN auch abhängige Komponenten (unter anderem Laufzeitumgebungen, Bibliotheken, Schnittstellen sowie weitere Programme) mitbetrachtet werden. Der IT-Betrieb MUSS in Abstimmung mit den Fachverantwortlichen festlegen, wer die Software wie installieren darf. Idealerweise SOLLTE Software immer zentral durch den IT-Betrieb installiert werden. Ist es erforderlich, dass die Software (teilweise) manuell installiert wird, dann MUSS der IT-Betrieb eine Installationsanweisung erstellen, in der klar geregelt wird, welche Zwischenschritte zur Installation durchzuführen und welche Konfigurationen vorzunehmen sind.

Darüber hinaus MUSS der IT-Betrieb regeln, wie die Integrität der Installationsdateien überprüft wird. Falls zu einem Installationspaket digitale Signaturen oder Prüfsummen verfügbar sind, MÜSSEN mit diesen die Integrität überprüft werden.

Sofern erforderlich, SOLLTE der IT-Betrieb eine sichere Standardkonfiguration der Software festlegen, mit der die Software konfiguriert wird. Die Standardkonfiguration SOLLTE dokumentiert werden.

APP.6.A5 Sichere Installation von Software (B)

Software MUSS entsprechend der Regelung für die Installation auf den IT-Systemen installiert werden. Dabei MÜSSEN ausschließlich unveränderte Versionen der freigegebenen Software verwendet werden.

Wird von diesen Anweisungen abgewichen, MUSS dies durch Vorgesetzte und den IT-Betrieb genehmigt werden und entsprechend dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.6.A6 Berücksichtigung empfohlener Sicherheitsanforderungen (S)

Die Institution SOLLTE die nachfolgenden Sicherheitsanforderungen im Anforderungskatalog für die Software berücksichtigen:

- Die Software SOLLTE generelle Sicherheitsfunktionen wie Protokollierung und Authentifizierung umfassen, die im Anwendungskontext erforderlich sind.

- Die Software SOLLTE es ermöglichen, die Härtungsfunktionen der Einsatzumgebung zu nutzen. Hierbei SOLLTEN insbesondere die Härtungsfunktionen des geplanten Betriebssystems und der geplanten Ausführungsumgebung berücksichtigt werden.
- Wenn durch die Software Informationen über ungesicherte, öffentliche Netze übertragen werden, dann SOLLTE die Software sichere Verschlüsselungsfunktionen einsetzen, die dem Stand der Technik entsprechen. Darüber hinaus SOLLTEN die übertragenen Daten auf Integrität überprüft werden, indem Prüfsummen oder digitale Signaturen eingesetzt werden.
- Verwendet die Software Zertifikate, dann SOLLTE sie die Möglichkeit bieten, die Zertifikate transparent darzustellen. Zudem SOLLTE es möglich sein, Zertifikate zu sperren, ihnen das Vertrauen zu entziehen oder eigene Zertifikate zu ergänzen.

Die sich aus den Sicherheitsanforderungen ergebenden Funktionen der Software SOLLTEN im Betrieb verwendet werden.

APP.6.A7 Auswahl und Bewertung potentieller Software (S) [Fachverantwortliche, Beschaffungsstelle]

Anhand des Anforderungskatalogs SOLLTEN die am Markt erhältlichen Produkte gesichtet werden. Sie SOLLTEN mithilfe einer Bewertungsskala miteinander verglichen werden. Danach SOLLTE untersucht werden, ob die Produkte aus der engeren Wahl die Anforderungen der Institution erfüllen. Gibt es mehrere Alternativen für Produkte, SOLLTEN auch die Akzeptanz der Benutzenden und der zusätzliche Aufwand für z. B. Schulungen oder die Migration berücksichtigt werden. Fachverantwortliche SOLLTEN gemeinsam mit dem IT-Betrieb anhand der Bewertungen und Testergebnisse ein geeignetes Softwareprodukt auswählen.

APP.6.A8 Regelung zur Verfügbarkeit der Installationsdateien (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit der Installationsdateien sicherstellen, um die Installation reproduzieren zu können. Hierzu SOLLTE der IT-Betrieb

- die Installationsdateien geeignet sichern oder
- die Verfügbarkeit der Installationsdateien durch die Bezugsquelle (z. B. App-Store) sicherstellen.

Zusätzlich SOLLTE sichergestellt werden, dass Software reproduzierbar konfiguriert werden kann. Hierzu SOLLTEN die Konfigurationsdateien gesichert werden. Alternativ SOLLTE geeignet dokumentiert werden, wie die Software konfiguriert wird.

Diese Regelung SOLLTE in das Datensicherungskonzept der Institution integriert werden.

APP.6.A9 Inventarisierung von Software (S)

Software SOLLTE inventarisiert werden. In einem Bestandsverzeichnis SOLLTE dokumentiert werden, auf welchen Systemen die Software unter welcher Lizenz eingesetzt wird. Bei Bedarf SOLLTEN zusätzlich die sicherheitsrelevanten Einstellungen miterfasst werden. Software SOLLTE nur mit Lizenzen eingesetzt werden, die dem Einsatzzweck und den vertraglichen Bestimmungen entsprechen. Die Lizenz SOLLTE den gesamten vorgesehenen Benutzungszeitraum der Software abdecken.

Wird von einer Standardkonfiguration abgewichen, SOLLTE dies dokumentiert werden. Das Bestandsverzeichnis SOLLTE anlassbezogen durch den IT-Betrieb aktualisiert werden, insbesondere wenn Software installiert wird.

Das Bestandsverzeichnis SOLLTE so aufgebaut sein, dass bei Sicherheitsvorfällen eine schnelle Gesamtübersicht mit den notwendigen Details ermöglicht wird.

APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software (S)

Die Institution SOLLTE die Regelungen, die festlegen, wie die Software eingesetzt und betrieben wird, in einer Sicherheitsrichtlinie zusammenfassen. Die Richtlinie SOLLTE allen relevanten Verantwortlichen, Zuständigen und Mitarbeitenden der Institution bekannt sein und die Grundlage für ihre Arbeit und ihr Handeln bilden. Inhaltlich SOLLTE die Richtlinie auch ein Benutzenden-Handbuch umfassen, dass erläutert, wie die Software zu benutzen und zu administrieren ist.

Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeitenden sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

APP.6.A11 Verwendung von Plug-ins und Erweiterungen (S)

Es SOLLTEN nur unbedingt notwendige Plug-ins und Erweiterungen installiert werden. Werden Erweiterungen eingesetzt, SOLLTE die Software die Möglichkeit bieten, Erweiterungen zu konfigurieren und abzuschalten.

APP.6.A12 Geregelte Außerbetriebnahme von Software (S) [Fachverantwortliche]

Wenn Software außer Betrieb genommen wird, SOLLTE der IT-Betrieb mit den Fachverantwortlichen regeln, wie dies im Detail durchzuführen ist. Ebenfalls SOLLTE geregelt werden, wie die Benutzenden hierüber zu informieren sind. Hierbei SOLLTE geklärt werden, ob die funktionalen Anforderungen fortbestehen (z. B. zur Bearbeitung von Fachaufgaben). Ist dies der Fall, dann SOLLTE geregelt werden, wie die benötigten Funktionen der betroffenen Software weiter verfügbar sein werden.

APP.6.A13 Deinstallation von Software (S)

Wird Software deinstalliert, SOLLTEN alle angelegten und nicht mehr benötigten Dateien entfernt werden. Alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden und nicht länger benötigt werden, SOLLTEN rückgängig gemacht werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.6.A14 Nutzung zertifizierter Software (H)

Bei der Beschaffung von Software SOLLTE festgelegt werden, ob Zusicherungen des herstellenden oder anbietenden Unternehmens über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden können. Ist dies nicht der Fall, SOLLTE eine Zertifizierung der Anwendung z. B. nach Common Criteria als Entscheidungskriterium herangezogen werden. Stehen mehrere Produkte zur Auswahl, SOLLTEN insbesondere dann Sicherheitszertifikate berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.14 „Security requirements of information systems“ Anforderungen an die Informationssicherheit von IT-Systemen, die auch bei der Auswahl und dem Einsatz von Software berücksichtigt werden sollten.

Die Common Criteria for Information Technology Security Evaluation (CC) stellen die Basis für international anerkannte Produktzertifizierungen dar. Eine CC-Zertifizierung kann somit als Nachweis für die Informationssicherheit eines Softwareproduktes herangezogen werden.

Das National Institute of Standardisation and Technology formuliert in der NIST Special Publication 800-53 im Appendix F „Family System and Service Acquisition“ unter anderem Anforderungen an die Anschaffung von IT-Produkten, hierunter auch Software.

Das Information Security Forum (ISF) stellt in seinem Standard „The Standard of Good Practice for Information Security“ in dem Kapitel „Business Application Management“ unter anderem Best Practices zur Absicherung von Software vor.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.7 Entwicklung von Individualsoftware

1. Beschreibung

1.1. Einleitung

Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit unangepasster Software lösen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen häufig Softwarelösungen, die auf die individuellen Bedürfnisse der Institutionen zugeschnitten sind. Im Folgenden werden diese Softwarelösungen als Individualsoftware bezeichnet. Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der Institution angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der Institution selbst oder von Dritten entwickelt werden. Hierzu gehören Anwendungen zur Geschäftsprozesssteuerung oder individuell angepasste Fachanwendungen, wie Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozialdaten oder Meldedaten.

Von essentieller Bedeutung ist es hierbei, dass bereits bei der Planung und Konzeptionierung der Individualsoftware auch die benötigten Sicherheitsfunktionen bedacht werden und die Informationssicherheit in dem gesamten Lebenszyklus der Individualsoftware berücksichtigt wird. Fehler in der Planung oder fehlende Sicherheitsfunktionen können im laufenden Betrieb nicht oder nur mit hohem zusätzlichem Aufwand ausgeglichen werden.

Individualsoftware wird dabei in der Regel im Rahmen eines Projektes entwickelt. Hierzu haben sich die unterschiedlichsten Vorgehens- bzw. Projektmanagementmodelle etabliert. Während klassische, lineare Vorgehensmodelle, wie der Wasserfallprozess, sehr gut zu Projekten mit zu Beginn feststehenden Anforderungen passen, ermöglichen agile Vorgehensmodelle, wie Scrum, Individualsoftware iterativ und inkrementell zu entwickeln. Agile Vorgehensmodell können sich somit besser an verändernde Gegebenheiten anpassen, insbesondere wenn zu Beginn noch nicht alle Anforderungen feststehen. Allerdings bieten sie nicht dieselbe Kalkulationssicherheit wie lineare Vorgehensmodelle und passen auch in einigen Fällen nicht zu den klassischen Strukturen der Beschaffungsprozesse, die auf ein lineares Vorgehen ausgerichtet sind.

1.2. Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche grundlegenden Sicherheitsanforderungen bei der Planung und Entwicklung von Individualsoftware zu berücksichtigen sind.

1.3. Abgrenzung und Modellierung

Der Baustein APP.7 *Entwicklung von Individualsoftware* ist für jede Entwicklung einer Individualsoftware einmal anzuwenden.

Aspekte zur Planung, Konzeption und Einsatz von Individualsoftware, wie benötigte Sicherheitsfunktionen festzulegen oder Individualsoftware außer Betrieb zu nehmen, werden im Baustein APP.6 *Allgemeine Software* behandelt. Er ist daher immer zusammen mit diesem Baustein anzuwenden.

Wenn Software entwickelt wird, liegt sehr häufig ein auftragnehmendes und auftraggebendes Verhältnis vor. Im IT-Grundschutz spiegelt sich dieser Sachverhalt wider, indem der Baustein APP.7 *Entwicklung von Individualsoftware* die auftragsgebende Seite und der Baustein CON.8 *Software-Entwicklung* die auftragnehmende Seite behandeln.

Die Freigabe und Tests von Individualsoftware wird im Baustein OPS.1.1.6 *Software-Tests und -Freigaben* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.7 *Entwicklung von Individualsoftware* von besonderer Bedeutung.

2.1. Unzulängliche vertragliche Regelungen mit externen Dienstleistenden

Aufgrund von unzulänglichen vertraglichen Regelungen mit externen Dienstleistenden können vielfältige und schwerwiegende Sicherheitsprobleme auftreten. Dies gilt insbesondere, wenn Anwendungen erstellt, eingeführt oder gewartet werden. Sind Aufgaben, Leistungsparameter oder der Aufwand ungenügend oder missverständlich beschrieben, können Sicherheitsmaßnahmen möglicherweise aus Unkenntnis oder aufgrund mangelnder Qualifizierung oder fehlender Ressourcen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa wenn regulatorische Anforderungen und Pflichten nicht erfüllt werden, Auskunftspflichten und Gesetze nicht eingehalten werden oder keine Verantwortung übernommen wird, weil Kontroll- und Steuerungsmöglichkeiten fehlen.

2.2. Software-Konzeptionsfehler

Werden Anwendungen, Programme und Protokolle konzeptioniert, können sicherheitsrelevante Konzeptionsfehler entstehen. Diese ergeben sich häufig daraus, dass Anwendungsmodule und Protokolle, die für einen bestimmten Zweck vorgesehen sind, in anderen Einsatzszenarien wiederverwendet werden. Sind dann andere Sicherheitsvorgaben relevant, kann dies zu massiven Sicherheitsproblemen führen, zum Beispiel wenn Anwendungsmodule und Protokolle, die eigentlich für abgeschottete betriebliche Umgebungen vorgesehen sind, an das Internet angebunden werden.

2.3. Undokumentierte Funktionen

Viele Anwendungen enthalten vom herstellenden Unternehmen eingebaute, undokumentierte Funktionen, häufig für die Entwicklung oder zum Support der Anwendung. Diese sind den Benutzenden meistens nicht bekannt. Undokumentierte Funktionen sind dann problematisch, wenn sie es erlauben, dass wesentliche Sicherheitsmechanismen umgangen werden, z. B. zum Zugriffsschutz. Dies kann die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten erheblich beeinträchtigen.

2.4. Fehlende oder unzureichende Sicherheitsmaßnahmen in Anwendungen

Sicherheitsmechanismen oder Sicherheitsfunktionen sollen in der Anwendung sicherstellen, dass bei der Verarbeitung von Informationen die Vertraulichkeit, Integrität und Verfügbarkeit im benötigten Maße gewährleistet werden können. Häufig steht bei der Entwicklung einer Anwendung aber die fachliche Funktionalität oder der Zeit- und Kostenrahmen im Vordergrund. So können wichtige Sicherheitsmechanismen zu schwach ausgeprägt sein, sodass sie einfach umgangen werden können oder sogar ganz fehlen.

2.5. Mangelhafte Steuerung der Software-Entwicklung

Wird die Software-Entwicklung vom Auftraggebenden nicht hinreichend gesteuert, bestehen eine Reihe von Gefahren, wie z. B.:

- Es können geforderte Sicherheitsfunktionen fehlen oder nur unzureichend implementiert werden. Hieraus können sich vielfältige Risiken ergeben, die die Verfügbarkeit, Vertraulichkeit und Integrität der mit der Individualsoftware verarbeiteten Daten gefährden.
- Das Entwicklungsprojekt kann sich zeitlich verzögern, sodass die Individualsoftware nicht rechtzeitig verfügbar ist.
- Prioritäten können falsch gesetzt werden, indem z. B. nachrangig benötigte Funktionen umfangreich entwickelt werden und dringend benötigte Sicherheitsfunktionen nur rudimentär implementiert werden. Auch hieraus können Projektverzögerungen und vielseitige Sicherheitsrisiken entstehen.

2.6. Beauftragung ungeeigneter Software-Entwickelnder

Werden ungeeignete Software-Entwickelnde beauftragt, können daraus unterschiedliche Gefährdungen entstehen:

- Aufgrund fehlender fachlicher Expertise, z. B. in der verwendeten Programmiersprache, in den eingesetzten Frameworks oder der geplanten technischen Einsatzumgebung, kann die Software viele vermeidbare Sicherheitslücken umfassen.
- Fehlende Kenntnisse im Bereich des Projektmanagements und Requirements Engineering können zu Reibungsverlusten in Abstimmungsprozessen und somit zu erheblichen Verzögerungen führen. Auch können deswegen Schwerpunkte falsch gesetzt werden und so wesentliche Sicherheitsfunktionen nicht mit der erforderlichen Priorität implementiert werden. Ungeeignete Software-Entwickelnde können beispielsweise aufgrund zu knapper, unrealistischer Kostenkalkulationen beauftragt werden. Auch Fehler, missverständliche Anforderungen und falsche Zielvorstellungen in Ausschreibungen können dazu führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.7 *Entwicklung von Individualsoftware* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	Beschaffungsstelle, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.7.A1 Erweiterung der Planung des Software-Einsatzes um Aspekte von Individualsoftware (B)

Die Planung des Software-Einsatzes MUSS um Aspekte von Individualsoftware ergänzt werden, indem definiert wird,

- wer dafür zuständig ist, die Software-Entwicklung bzw. den Auftragnehmenden zu steuern und zu koordinieren, sowie
- in was für einen organisatorischen Rahmen die Software zu entwickeln ist (Projektmanagementmodell).

Individualsoftware SOLLTE im Rahmen eines Entwicklungsprojektes entwickelt werden. Das Entwicklungsprojekt sollte anhand eines Ablaufplans zeitlich grob geplant werden.

APP.7.A2 Festlegung von Sicherheitsanforderungen an den Prozess der Software-Entwicklung (B)

Die Institution MUSS klare Anforderungen an den Prozess der Software-Entwicklung definieren. Aus den Anforderungen MUSS hervorgehen, in was für einer Umgebung die Software entwickelt werden darf und welche technischen und organisatorischen Maßnahmen von Seiten der beauftragten Software-Entwickelnden umzusetzen sind.

APP.7.A3 Festlegung der Sicherheitsfunktionen zur Systemintegration (B) [IT-Betrieb]

Der IT-Betrieb und die zuständigen Fachverantwortlichen MÜSSEN Anforderungen an die technische Einsatzumgebung der geplanten Individualsoftware erstellen und mit der Software-Entwicklung abstimmen. Aus den Anforderungen MUSS klar hervorgehen:

- auf was für einer Hardware-Plattform,
- auf was für einer Software-Plattform (inklusive gesamten Software-Stack),
- mit welchen zur Verfügung stehenden Ressourcen (z. B. CPU-Cluster oder Arbeitsspeicher),
- mit welchen Schnittstellen mit anderen IT-Systemen oder Anwendungen sowie
- mit welchen sich hieraus ergebenen Sicherheitsfunktionen

die Anwendung eingesetzt werden soll. Schnittstellen mit anderen IT-Systemen SOLLTEN in standardisierten technischen Formaten modelliert und definiert werden.

APP.7.A4 Anforderungsgerechte Beauftragung (B) [Beschaffungsstelle]

Wird Individualsoftware durch die eigene Institution entwickelt oder extern beauftragt, dann MÜSSEN neben den bestehenden rechtlichen und organisatorischen Vorgaben insbesondere

- der Anforderungskatalog (siehe hierzu APP.6 *Allgemeine Software*),
- die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie
- die Sicherheitsfunktionen zur Systemintegration

als Grundlage zur Software-Entwicklung verwendet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.7.A5 Geeignete Steuerung der Anwendungsentwicklung (S)

Bei der Entwicklung von Individualsoftware SOLLTE ein geeignetes Steuerungs- und Projektmanagementmodell verwendet werden. Hierbei SOLLTE das ausgewählte Modell mit dem Auftragnehmenden abgestimmt werden. Bei der Steuerung SOLLTE es berücksichtigt werden.

Es SOLLTE insbesondere berücksichtigt werden, dass das benötigte Personal ausreichend qualifiziert ist. Alle relevanten Phasen SOLLTEN während des Lebenszyklus der Software abgedeckt werden. Außerdem SOLLTE es ein geeignetes Entwicklungsmodell, ein Risikomanagement sowie Qualitätsziele enthalten.

APP.7.A6 Dokumentation der Anforderungen an die Individualsoftware (S)

Die Anforderungen aus den Anforderungskatalog, die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie die Sicherheitsfunktionen zur Systemintegration SOLLTEN umfassend dokumentiert werden. Insbesondere SOLLTE ein Sicherheitsprofil für die Anwendung erstellt werden. Dieses SOLLTE den Schutzbedarf der zu verarbeiteten Daten und Funktionen dokumentieren. Die Dokumentation mitsamt Sicherheitsprofil SOLLTE den Entwickelnden zur Software-Entwicklung zur Verfügung gestellt werden.

Die Dokumentation SOLLTE bei Änderungen an der Individualsoftware sowie bei funktionalen Updates aktualisiert werden.

APP.7.A7 Sichere Beschaffung von Individualsoftware (S)

Das Entwicklungsprojekt SOLLTE im Rahmen des hierfür bestens geeigneten Projektmanagementmodells beauftragt werden. Sicherheitsaspekte SOLLTEN dabei bereits bei der Ausschreibung und Vergabe berücksichtigt werden, sodass

- einerseits nur geeignete Auftragnehmende beauftragt werden,
- andererseits aber keine weitreichenden Rückschlüsse auf die Sicherheitsarchitektur durch die öffentlich verfügbaren Informationen möglich sind.

In der Institution SOLLTEN definierte Prozesse und festgelegte Kontaktpersonen existieren, die sicherstellen, dass die jeweiligen Rahmenbedingungen berücksichtigt werden.

APP.7.A8 Frühzeitige Beteiligung der Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests (S)

Fachverantwortliche SOLLTEN schon vor der endgültigen Abnahme frühzeitig an entwicklungsbegleitenden Tests der Software-Entwickelnden beteiligt werden. Dies SOLLTE in Abstimmung mit dem Auftragnehmenden bereits initial im Projektablaufplan berücksichtigt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.7.A9 Treuhänderische Hinterlegung (H)

Für institutionskritische Anwendungen SOLLTE geprüft werden, ob diese gegen Ausfall des herstellenden Unternehmens abgesichert werden. Dafür SOLLTEN nicht zum Lieferumfang der Anwendung gehörende Materialien und Informationen treuhänderisch hinterlegt werden, etwa bei einer Escrow-Agentur. Dokumentierter Code, Konstruktionspläne, Schlüssel oder Passwörter SOLLTEN dazu gehören. Die Pflichten der Escrow-Agentur zur Hinterlegung und Herausgabe SOLLTEN vertraglich geregelt werden. Es SOLLTE geklärt werden, wann das Hinterlegte an wen herausgegeben werden darf.

APP.7.A10 Beauftragung zertifizierter Software-Entwicklungsunternehmen (H)

Werden besonders sicherheitskritische Anwendungen entwickelt, SOLLTEN hierzu zertifizierte Software-Entwicklungsunternehmen beauftragt werden. Die Zertifizierung SOLLTE Sicherheitsaspekte für relevante Aspekte der Software-Entwicklung umfassen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt

- in der Norm ISO/IEC 12207:2008, „System and software engineering – Software life cycle process“ einen Überblick über alle Bestandteile des Lebenszyklus einer Software,
- in der Norm ISO/IEC 15408-2:2008, „Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components“ einen Überblick über die Möglichkeiten der Systemabsicherung und
- in der Norm ISO/IEC 27001:2013, „Information technology – Security technigues – Information security management systems – Requirements“ im Annex A, A.14 System acquisition, development and maintenance“ Anforderungen an die System-Entwicklung und den -betrieb.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in der „Area BA Business Application Management“ Anforderungen an das Management von Business-Anwendungen.

Das National Institute of Standards and Technology stellt in der „NIST Special Publication 800-53“ im Apendix F-SA „Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity“ weitergehende Anforderungen an den Umgang mit Individualsoftware.

SYS: IT-Systeme

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.1 Allgemeiner Server

1. Beschreibung

1.1. Einleitung

Als „Allgemeiner Server" werden IT-Systeme mit einem beliebigen Betriebssystem bezeichnet, die Benutzenden und anderen IT-Systemen Dienste bereitstellen. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, oder auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server-IT-Systeme haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben im Hintergrund, ohne dass Benutzende direkt mit ihnen im Austausch stehen. Auf der anderen Seite gibt es Serverdienste, die direkt mit den Benutzenden interagieren und nicht auf den ersten Blick als Serverdienst wahrgenommen werden. Ein bekanntes Beispiel sind X-Server unter Unix.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Servern verarbeitet, angeboten oder darüber übertragen werden, sowie der Schutz der damit zusammenhängenden Dienste.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.1 *Allgemeiner Server* ist auf alle Server-IT-Systeme mit beliebigem Betriebssystem anzuwenden.

In der Regel werden Server unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind im IT-Grundschutz-Kompendium eigene Bausteine vorhanden, die auf dem vorliegenden Baustein aufbauen. Der Baustein SYS.1.1 *Allgemeiner Server* bildet die Grundlage für die Bausteine der konkreten Server-Betriebssysteme. Sofern für ein betrachtetes IT-System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein SYS.1.1 *Allgemeiner Server* anzuwenden. Falls für eingesetzte Server-Betriebssysteme kein spezifischer Baustein existiert, müssen die Anforderungen des vorliegenden Bausteins geeignet für das Zielobjekt konkretisiert und es muss eine ergänzende Risikobetrachtung durchgeführt werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Serverdienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die Bereitstellung von Benutzendensitzungen durch Terminalserver ist ebenfalls als Dienst zu betrachten. Für Terminalserver ist entsprechend der Baustein SYS.1.9 *Terminalserver* zu modellieren.

Grundsätzlich sind die Anforderungen an das Rollen- und Berechtigungskonzept aus dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu berücksichtigen. Ebenfalls zu berücksichtigen sind Anforderungen aus dem Baustein DER.4 *Notfallmanagement*.

Server sollten grundsätzlich beim Konzept zum Schutz vor Schadsoftware berücksichtigt werden. Anforderungen dazu finden sich im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen*.

Bei Servern gibt es besondere Anforderungen an die Administration sowie den Umgang mit Patches und Änderungen. Deswegen sind die Anforderungen der Bausteine OPS.1.1.2 *Ordnungsgemäße IT-Administration* und OPS1.1.3 *Patch- und Änderungsmanagement* zu beachten.

Server bieten häufig Dienste für eine Vielzahl von Clients an, oft auch über das Internet. Aus diesem Grund sind sie besonders vom übrigen Netz der Institution zu trennen. Anforderungen dazu gibt es im Baustein NET.1.1 *Netzarchitektur und -design*.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.1 *Allgemeiner Server* von besonderer Bedeutung.

2.1. Unzureichende Planung

Server sind komplexe IT-Systeme mit einer großen Anzahl an Funktionen und Konfigurationsoptionen. Auch wenn moderne Server-Betriebssysteme in vielen Bereichen gute Standardeinstellungen mitbringen, ist die Grundkonfiguration immer noch nicht in jedem Fall die sicherste. Dies kann bei unzureichender Planung zu einer Vielzahl von Schwachstellen und Schwächen durch Fehlkonfiguration führen, die von unberechtigten Dritten leicht ausgenutzt werden können. Werden außerdem nicht schon vor der Installation zentrale Entscheidungen getroffen, werden Server oft in einem unsicheren und undefinierten Zustand ausgeführt, der sich nachträglich kaum mehr beheben lässt.

2.2. Fehlerhafte Administration von Servern

Neue Versionen von Server-Betriebssystemen werden im Vergleich zu den Vorgängerversionen regelmäßig um neue Funktionen erweitert. Auch bei bereits vorhandenen Features können sich Teilfunktionen, Parameter oder Standardkonfigurationen in neuen Versionen verändern. Ist der IT-Betrieb der Institution nicht ausreichend in den Besonderheiten der Betriebssysteme geschult, drohen Konfigurationsfehler und menschliche Fehlhandlungen, die neben der Funktionalität auch die Sicherheit des IT-Systems beeinträchtigen können.

Eine besondere Gefahr stellen uneinheitliche Server-Sicherheitseinstellungen dar (z. B. bei SMB, RPC oder LDAP). Wenn die Konfiguration nicht systematisch und zentral geplant, dokumentiert, überprüft und nachgehalten wird, droht ein sogenannter Konfigurationsdrift. Je mehr sich die konkreten Konfigurationen funktional ähnlicher Systeme unbegründet und undokumentiert auseinander bewegen, desto schwieriger wird es, einen Überblick über den Status quo zu behalten und die Sicherheit ganzheitlich und konsequent aufrechtzuerhalten.

2.3. Unberechtigtes Erlangen oder Missbrauch von Administrationsrechten

Die reguläre Arbeit mit Administrationsrechten, wie beispielsweise die Erledigung von Aufgaben und Tätigkeiten, die auf einem Client-System grundsätzlich mit Standardberechtigungen vorgesehen und möglich sind, stellt auf einem Server ein Sicherheitsrisiko dar. Sind gesonderte administrative Konten nicht auf die minimal notwendigen Rechte zur Durchführung administrativer Tätigkeiten beschränkt („Least Privilege"-Prinzip), können bei Übernahme solcher Konten weitreichende Rechte auf dem Server oder weiteren IT-Systemen erlangt und hoher Schaden verursacht werden. Auch ein Missbrauch von Rechten durch legitime Administrierende ist ein relevantes Schadensszenario. Da die Rollen oft sehr mächtig sind, sind hier die Auswirkungen in der Regel beträchtlich, etwa bei den sogenannten Domänenadministratoren. Auch ohne Passwörter zu erraten oder zu brechen, können z. B. durch sogenannte Pass-the-Hash-Verfahren geeignete Credentials ausgelesen und missbraucht werden, um sich lateral im Netz weiterzubewegen.

2.4. Datenverlust

Der Verlust von Daten kann besonders bei Servern erhebliche Auswirkungen auf Geschäftsprozesse und Fachaufgaben und damit auf die gesamte Institution haben. Sehr viele IT-Systeme wie Clients oder andere Server sind in der Regel darauf angewiesen, dass die dort zentral gespeicherten Daten immer verfügbar sind.

Wenn institutionsrelevante Informationen, egal welcher Art, zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar deren Ausführung verhindert werden. Insgesamt kann der Verlust gespeicherter Daten, neben dem Ausfall und den Kosten für die Wiederbeschaffung der Daten, vor allem zu langfristigen Konsequenzen wie Vertrauenseinbußen in Geschäftsbeziehungen, zu juristischen Auswirkungen sowie zu einem negativen Eindruck in der Öffentlichkeit führen. In vielen Institutionen existieren Regelungen, dass keine Daten auf den lokalen Clients gespeichert werden dürfen, sondern stattdessen zentrale Ablagen auf den Servern dazu genutzt werden müssen. Ein Verlust dieser zentral abgelegten Daten hat in einem solchen Fall gravierende Auswirkungen. Durch die verursachten direkten und indirekten Schäden können Institutionen sogar in ihrer Existenz bedroht sein.

2.5. Denial-of-Service-Angriffe

Ein Angriff auf die Verfügbarkeit von Datenbeständen, der „Denial of Service" genannt wird, zielt darauf ab, zu verhindern, dass benötigte und normalerweise verfügbare Funktionen oder Geräte verwendet werden können. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen. Indem diese Ressourcen bei Angriffen sehr stark in Anspruch genommen werden, kann nicht mehr regulär darauf zugegriffen werden. In der Regel sind IT-Systeme auch stark voneinander abhängig. Somit sind von der Verknappung der Ressourcen eines Servers schnell weitere Server betroffen. Es können zum Beispiel CPU-Zeit, Speicherplatz oder Bandbreite künstlich verknappt werden. Dies kann dazu führen, dass Dienste oder Ressourcen überhaupt nicht mehr genutzt werden können.

2.6. Bereitstellung unnötiger Applikationen und Dienste

Schon bei der Installation des Server-Betriebssystems ist es möglich, mitgelieferte Applikationen und Dienste zu installieren, von denen einige unter Umständen gar nicht genutzt werden. Auch im späteren Betrieb wird oft Software installiert, die kurz getestet, aber danach nicht mehr benötigt wird. Oft ist gar nicht bekannt, dass diese nicht genutzten Anwendungen und Dienste vorhanden sind. Auf diese Weise befinden sich zahlreiche Applikationen und Dienste auf den Servern, die nicht eingesetzt werden und die ihn so unnötig belasten.

Außerdem können diese nicht genutzten Anwendungen und Dienste Schwachstellen enthalten, etwa wenn sie nicht mehr aktualisiert werden. Sind die installierten Anwendungen und Dienste unbekannt, ist der Institution gar nicht bewusst, dass diese ebenfalls aktualisiert werden müssen. Auf diese Weise können sie leicht zum Einfallstor für Angriffe werden.

2.7. Überlastung von Servern

Wenn Server nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, an dem sie den Anforderungen der Institution nicht mehr gerecht werden. Je nach Art der betroffenen IT-Systeme kann dies eine Vielzahl von negativen Auswirkungen haben. So können die Server oder Dienste beispielsweise vorübergehend nicht verfügbar sein oder es können Datenverluste auftreten. Die Überlastung eines einzelnen Servers kann bei komplexen IT-Landschaften außerdem dazu führen, dass bei weiteren Servern Probleme oder Ausfälle auftreten.

Auslöser für die Überlastung von IT-Systemen kann sein, dass

- installierte Dienste oder Anwendungen falsch konfiguriert sind und so unnötig viel Speicher beanspruchen,
- vorhandene Speicherplatzkapazitäten überschritten werden,
- zahlreiche Anfragen zur gleichen Zeit ein IT-System überbeanspruchen,
- zu viel Rechenleistung von den Diensten beansprucht wird oder
- eine zu große Anzahl an Nachrichten zur gleichen Zeit versendet wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.1.A1 Zugriffsschutz und Nutzung (B)

Physische Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Physische Server MÜSSEN daher in Rechenzentren, Serverräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden (siehe hierzu die entsprechenden Bausteine der Schicht INF *Infrastruktur*). Bei virtualisierten Servern MUSS der Zugriff auf die Ressourcen der Instanz und deren Konfiguration ebenfalls auf die berechtigten Personen begrenzt werden.

Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden. Server DÜRFEN NICHT zur Erledigung von Aufgaben und Tätigkeiten verwendet werden, die grundsätzlich auf einem Client-System aus- und durchgeführt werden können. Insbesondere DÜRFEN vorhandene Anwendungen, wie Webbrowser, auf dem Server NICHT für das Abrufen von Informationen aus dem Internet oder das Herunterladen von Software, Treibern und Updates verwendet werden.

Als Arbeitsplatz genutzte IT-Systeme DÜRFEN NICHT als Server genutzt werden.

SYS.1.1.A2 Authentisierung an Servern (B)

Für die Anmeldung von Benutzenden und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale, netzbasierte Authentisierungsdienste zurückgegriffen werden.

SYS.1.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.1.A5 Schutz von Schnittstellen (B)

Es MUSS gewährleistet werden, dass nur dafür vorgesehene Wechselspeicher und sonstige Geräte an die Server angeschlossen werden können. Alle Schnittstellen, die nicht verwendet werden, MÜSSEN deaktiviert werden.

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste (B)

Alle nicht benötigten Serverrollen, Features und Funktionen, sonstige Software und Dienste MÜSSEN deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden. Die Empfehlungen des Betriebssystemherstellers SOLLTEN hierbei als Orientierung berücksichtigt werden.

Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzenden, aber auch für Anwendungen, geeignet beschränkt werden.

Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die Server gewählt wurden.

SYS.1.1.A7 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.1.A8 ENTFALLEN (B)

Diese Anforderung ist entfallen.